DATA SHEET

Thunder TPS

DDoS Detection and Mitigation with Intelligent Automation

A10 Thunder® Threat Protection System (TPS) is the scalable and automated DDoS protection solution powered by advanced machine learning leading the industry in precision, scalability, and performance.

Surgical Multi-vector DDoS Protection

Ensuring availability of business services requires organizations to rethink how to build scalable DDoS defenses that can surgically distinguish an attacker from a legitimate user.

New threat vectors have changed the breadth, intensity, and complexity of options available to attackers. Today's attacks have evolved, and now include DDoS toolkits, weaponized IoT devices, online DDoS services, and more. Established solutions, which rely on ineffective signature-based IPS or only traffic rate-limiting, are no longer adequate.

Thunder TPS scales to defend against the DDoS of Things and traditional zombie botnets and detects DDoS attacks through high-resolution packets or flow-record analysis from edge routers and switches. Unlike outdated DDoS defense products, A10 Networks' defenses include detection capabilities across key network elements including A10 Thunder® ADC, CGN and CFW. These capabilities provide the context, packet-level granularity and visibility needed to thwart today's sophisticated attacks. The One-DDoS protection detectors work in concert with A10 Networks aGalaxy® centralized management system and Thunder TPS for centralized mitigation to deliver fast and cost-effective DDoS resilience.

Thunder TPS' scale and zero-touch intelligent automation architecture with aGalaxy maximize ROI and help service providers enable profitable DDoS scrubbing services.

A10 Networks is available when you need help most. A10 support provides 24x7x365 services, including the A10 DDoS Security Incident Response Team (DSIRT) to help you understand and respond to DDoS incidents and orchestrate cloud scrubbing. A10 Threat Intelligence Service leverages global knowledge to proactively stop bad actors.

Platforms

Physical and SPE Appliances

Virtual Appliance

Cloud

Management

aGalaxy

Subscriber Portal

Services

DSIRT & DDoS Threat Intelligence

Talk with A10

A10networks.com/tps

Benefits

Maintain

Service Availability

Downtime results in immediate productivity and revenue loss for any business. Thunder TPS ensures service availability by automatically spotting anomalies across the traffic spectrum and mitigating multi-vector DDoS attacks.

Defeat

Growing Attacks

Thunder TPS protects the largest, most-demanding network environments. Thunder TPS offloads common attack vectors to specialized hardware, allowing its powerful multicore CPUs to distinguish legitimate users from attacking botnets and complex application-layer attacks that require resource-intensive deep packet inspection (DPI).

Scalable

Protection

Select Thunder TPS hardware models benefit from our Security and Policy Engine (SPE) hardware acceleration, leveraging FPGA-based FTA technology and other hardware-optimized packet processing for highly scalable flow distribution and hardware DDoS protection capabilities.

Deploy

Wartime Support

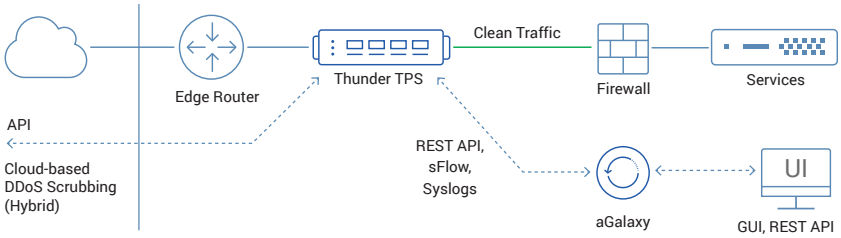
No organization has unlimited trained personnel or resources during real-time DDoS attacks. Thunder TPS supports five levels of programmatic mitigation escalation and de-escalation per protected zone. Remove the need for frontline personnel to make time-consuming manual changes to escalating mitigation strategies and improve response times during attacks. Administrators have the option to manually intervene and coordinate with A10's DSIRT at any stage of an attack.

Reduce

Security OPEX

Thunder TPS is extremely efficient. It delivers high performance in a small form factor to reduce OPEX with significantly lower power usage, rack space, and cooling requirements.

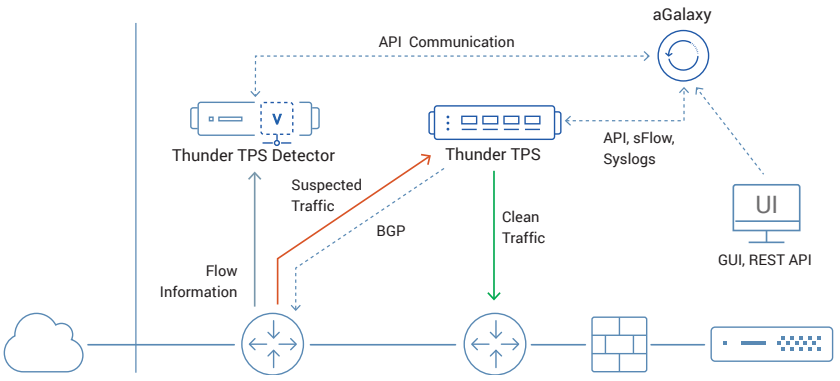
Reference Architectures



Proactive Deployment

(Asymmetric or Symmetric)

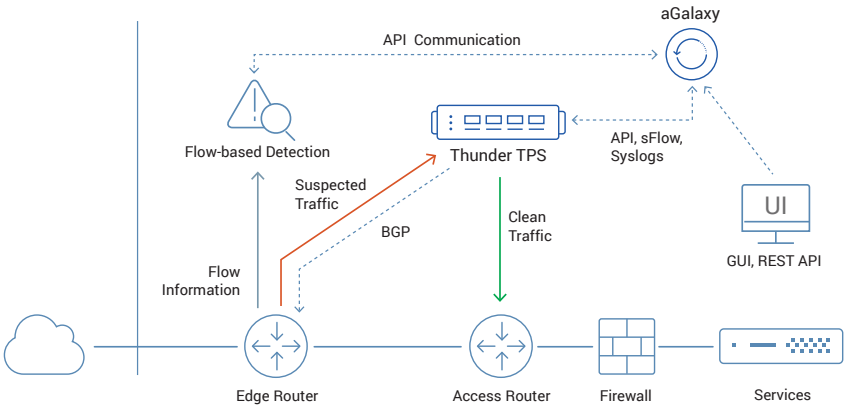
Deploying Thunder TPS in proactive mode provides continuous, comprehensive detection and fast mitigation. This mode is most useful for real-time environments where the user experience is critical, and for protection against application-layer attacks. Thunder TPS supports L2 or L3 inpath deployments. It also eases deployment of hybrid DDoS protection using a cloud scrubbing service in case volumetric attacks exceed an organization's internet bandwidth.



Reactive Deployment

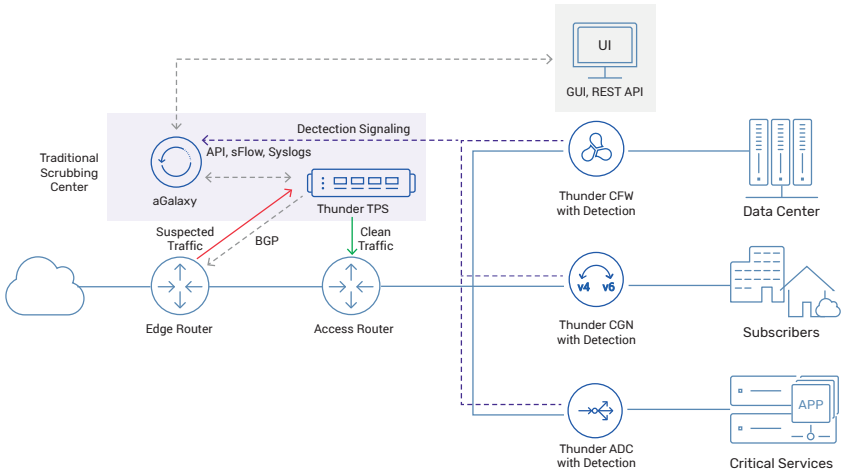
Larger networks benefit from on-demand mitigation, triggered manually or by flow analytical systems. Thunder TPS Detector is available as a standalone appliance (hardware or virtual). The flow-based DDoS detector supports tightly integrated interworking with aGalaxy management and Thunder TPS mitigation for a completely automated DDoS defense solution.

Reference Architectures



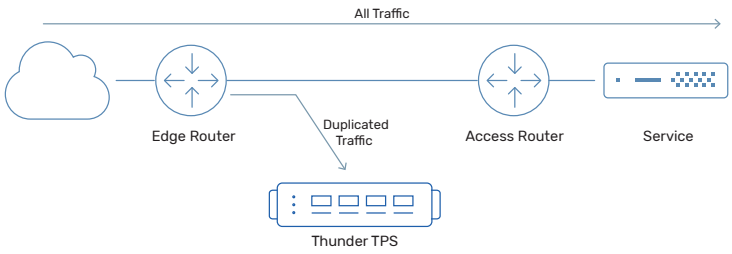
Reactive Deployment with Third-party Flow Detector

Thunder TPS fits in any network configuration with integrated BGP and other routing protocols. This eliminates the need for any additional diversion and re-injection routers. A10 Networks partners with the industry's leading network monitoring and DDoS detection companies to provide additional flexibility for creating best-of-class solutions for each customer's unique business needs. The third-party DDoS detection can leverage API (A10's aXAPI® and aGAPI®) or syslog, to create tightly integrated DDoS protection solutions.



Distributed Detection with One-DDoS Protection

One-DDoS protection provides full spectrum DDoS protection by placing detection capabilities across key network elements including A10's Thunder ADC, CGN and CFW. These capabilities provide the context, packet-level granularity and visibility needed to thwart today's sophisticated targeted attacks. The distributed DDoS detectors work in concert with aGalaxy and Thunder TPS for centralized mitigation that delivers fast and cost effective DDoS resilience.



Out-of-band (TAP) Mode

The out-of-band mode is used when packet-based DDoS detection and monitoring are required.

Features

Full Spectrum DDoS Protection for Service Availability

A10 Thunder TPS detects and mitigates broad levels of attacks, even if multiple attacks hit the network simultaneously.

Complete Solution

For Flexible Deployments

Thunder TPS provides a complete solution for DDoS defenses in proactive always-on or on-demand reactive modes to meet customers' business objectives. Thunder TPS can be deployed in L2 or L3 inpath modes with full IPv4 and IPv6 support. On-demand reactive DDoS detection is facilitated with the collection and analysis of exported flow data records from routers and switches. The Thunder TPS detector applies always-on adaptive learning to build peacetime profiles for protected servers and services based on 15 flow record traffic indicators to spot anomalous behavior. When an attack is detected, aGalaxy instructs Thunder TPS to initiate a BGP route redirection for the suspicious traffic. Then Thunder TPS applies the appropriate countermeasures using a progressive auto-mitigation level escalation technique before delivering the clean traffic to the intended destination.

Multi-vector

Attack Protection

Detect and mitigate DDoS attacks of many types, including volumetric, protocol, or resource attacks; application-level attacks; or IoT-based attacks. Hardware acceleration offloads the CPUs and makes Thunder TPS particularly adept to deal with simultaneous multi-vector attacks.

Hybrid

DDoS Protection

Thunder TPS on-premises protection works in concert with third-party cloud-based DDoS scrubbing services to provide full-spectrum protection against attacks of any type.

When attacks grow beyond an organization's bandwidth capacity, cloud mitigation can be initiated automatically by Thunder TPS using BGP-based signaling, API, and scripting, etc.

ZAP

Zero-day Automated Protection

The Zero-day Automated Protection (ZAP) utilizes heuristic and machine learning to automatically discover mitigation filters without advanced configuration or manual intervention. ZAP speeds the response time against increasingly sophisticated multi-vector attacks while minimizing downtime and errors and lower operating costs.

Non-stop DNS

Authoritative DNS Cache

A10 Thunder TPS can be configured as a high-performance DNS authoritative cache, enabling Thunder TPS' non-stop DNS operational mode to cache up to 240 million DNS records and respond to queries at rates of up to 70 million queries per second. Non-stop DNS can also work in conjunction with Thunder TPS DDoS defenses to create a highly resilient DNS service.

One-DDoS Protection

Layered, Distributed Detection

One-DDoS protection provides the freshest approach to full-spectrum DDoS defense, placing detection capabilities across key network portions closest to the targeted portions of the infrastructure. This provides the context, packet-level granularity, and visibility needed to thwart today's sophisticated targeted attacks.

A10 Thunder ADC, CGN, and CFW with integrated DDoS detectors work in concert with Thunder TPS' edge flow-based detection and centralized mitigation to enable full spectrum DDoS resilience.

A10 DDoS Threat Intelligence

Larger networks benefit from on-demand mitigation, triggered manually or by flow analytical systems. Thunder TPS Detector is available as a standalone appliance (hardware or virtual). The flow-based DDoS detector supports tightly integrated interworking with aGalaxy management and Thunder TPS mitigation for a complete reactive DDoS defense solution.

High Performance and Efficiency to Meet Growing Attack Scale

Thunder TPS provides solutions to protect organizations from attacks of all sizes, from 1 to 380 Gbps (or 3 Tbps in a list synchronization cluster).

High Performance

Protection

Select Thunder TPS models have high-performance FPGA-based Flexible Traffic Acceleration (FTA) technology to immediately detect and mitigate up to 60 common attack vectors in hardware -- before data CPUs are involved. Thunder TPS supports protocol and packet anomaly check and blocking of up to 500 million packets per second (Mpps). Thunder TPS enforces highly granular traffic rates up to 100 ms intervals. The enhanced vThunder TPS running on ESXi hypervisor provides 100 Gbps throughput in a single virtual appliance and can be expanded to 800 Gbps with eight-way clustering.

Simultaneous

Protected Objects

To protect entire networks, applications, and services, Thunder TPS simultaneously mitigates up to 3,000 zones with individual protection policies that include thousands of hosts, subnets, and services per zone. The scale of simultaneous mitigation helps organizations apply granular controls to protected objects and create profitable DDoS scrubbing services.

Complex

Attack Mitigation at Scale

Thunder TPS tracks more than 27 traffic and behavioral indicators and can apply escalating protocol challenges to surgically differentiate attackers from valid users for appropriate mitigation of up to 256 million concurrent tracked sessions.

Complex application attacks (e.g., HTTP, DNS, etc.) are mitigated with advanced parallel processing across a large number of CPU cores to maintain high-performance system scaling, even for multi-vector attacks.

Large Threat

Intelligence Class Lists

Eight lists, each containing up to 16 million entries, may be defined to utilize data from intelligence sources, such as the A10 DDoS Threat Intelligence Service, in addition to dynamically generated entries of actionable black/white lists.

Zero-day

Attack Pattern Recognition

DDoS attackers continue to innovate their multi-vector attack arsenals with new strategies. The Thunder TPS Zero-day Attack Pattern Recognition (ZAPR) engine automatically identifies DDoS attack characteristics and dynamically applies mitigation filters without advanced configuration or manual intervention.

Full Control and Smart Automation for Agile Protection

For network operators, it is critical that a DDoS mitigation solution integrates easily into many network architectures.

Efficient

Intelligent Automation

No organization has unlimited resources or the time for manual interventions. A10 provides the industry's most advanced intelligent automation capabilities powered by machine learning throughout the entire protection lifecycle.

Operators define the networks to protect and A10 defenses do the rest based on the operator's pre-defined policies, including individual learned detection threshold per monitored entity, automatic traffic redirection orchestration, start of mitigation and escalation, and then extract and apply attack pattern filters. When the attack subsides, the network and defenses are returned to peacetime posture and detailed reports are generated for future analysis.

Easy

Network Integration

With multiple performance options and flexible deployment models, Thunder TPS may be integrated into any network architecture of any size, including MPLS. And with aXAPI, A10's 100-percent programmable RESTful API, Thunder TPS easily integrates into third-party detection solutions and into agile SecOps workflows.

Leveraging open standards like BGP blackhole and Flowspec functionality, Thunder TPS mitigation integrates easily with any DDoS detection solution. Open APIs and networking standards enable tight integration with other devices, including A10 threat detection partners, SDN controllers, and other security products.

Effective

Management

Thunder TPS supports an industry-standard CLI, on-box GUI, and the aGalaxy management system. The CLI allows sophisticated operators easy troubleshooting and debugging. The intuitive on-box GUI enables ease of use and basic graphical reporting. aGalaxy offers a comprehensive dashboard with advanced reporting, mitigation console, and policy enforcement for multiple TPS devices.

aGalaxy is available with an optional integrated Thunder TPS detector that supports tightly integrated interworking of Thunder TPS DDoS mitigation, flow-based DDoS detection, system-wide management, and robust reporting.

Thunder
7655S TPS
by the Numbers

1.2 Tbps HW Blocking	380 Gbps Throughput	3 Tbps Throughput in Cluster	8x16M Threat Class Lists
100 GE Ports	500 Mpps Anomaly Drop (HW assisted)	60 Hardware Mitigations	64K Protected Objects

Thunder TPS Physical Appliance Specifications

Performance	Thunder 1040 TPS		Thunder 3040 TPS	Thunder 5845-40G TPS	Thunder 5845 TPS
Throughput (software scrubbing)*1	5 Gbps		10 Gbps	40 Gbps	100 Gbps
Hardware Blocking	N/A		N/A	250 Gbps	250 Gbps
Packets Rate (pps)*1	2.2 Million		4 Million	12 Million	25 Million
Software-based - SYN Authentication (pps)	2.2 Million		4 Million	12 Million	25 Million
Hardware-based - Anomaly Flood Blocking (pps)	N/A		N/A	125 Million	125 Million
Maximum Concurrent Sessions (asymmetric deployment)	8 Million		8 Million	32 Million	48 Million
Average Latency	10 µs		10 µs	50 µs	50 µs
Minimum Rate Enforcement Interval	100 ms		100 ms	100 ms	100 ms
Flow Detection Performance					
Flows Per Second (fps)	N/A		1 Million	3 Million	3 Million
Network Interface		Hardware Bypass Model			
1 GE Copper	5	1 + 4 (Bypass)	6	0	0
1 GE Fiber (SFP)	0	0	2	0	0
1/10 GE Fiber (SFP+)	4*3	4*3	4	48	48
1/10 GE Fiber (Fixed)	0	2 (Optical bypass)*5	0	0	0
100 GE Fiber	0	0	0	4 (QSFP28)	4 (QSFP28)
Management Ports	Ethernet Mgmt Port, RJ-45 Console Port				
Hardware Specifications					
Processor	Intel Communications Processor		Intel Xeon 4-core	Intel Xeon 18-core*6	Intel Xeon 18-core
Memory (ECC RAM)	16 GB		16 GB	64 GB *6	64 GB
Storage	SSD		SSD	SSD	SSD
Hardware Acceleration	Software		Software	2 x FTA-4, SPE	2 x FTA-4, SPE
Dimensions (inches)	1.75 (H) x 17.5 (W) x 17.25 (D)		1.75 (H) x 17.5 (W) x 17.45 (D)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 30 (D)
Rack Units (mountable)	1U		1U	1U	1U
Unit Weight	14 lbs | 16 lbs (RPS)		20.6 lbs	34.3 lbs	34.3 lbs
Power Supply (DC option available)	Single 750W*4		Dual 600W RPS	Dual 1500W RPS	Dual 1500W RPS
	80 Plus Platinum efficiency, 100-240 VAC, 50-60 Hz				
Power Consumption (typical/max)*2	80W / 110W		180W / 240W	585W / 921W	585W / 921W
Heat in BTU/Hour (typical/max)*2	273 / 376		615 / 819	1,997 / 3,143	1,997 / 3,143
Cooling Fan (front-to-back airflow)	Hot Swap Smart Fans				
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%				
Regulatory Certifications	FCC Class A, UL, CE, CB, VCCI, BSMI, RCM | RoHS		FCC Class A, UL, CE, CB, VCCI, KCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, CB, VCCI, KCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, CB, VCCI, KCC, BSMI, RCM | RoHS
Standard Warranty	90-day Hardware and Software				

Thunder TPS Physical Appliance (cont.)

Performance	Thunder 7445 TPS	Thunder 14045 TPS Single-Module	Thunder 14045 TPS Dual-Module	Thunder 7655S TPS
Throughput (software scrubbing)*1	220 Gbps	150 Gbps	300 Gbps	380 Gbps
Hardware Blocking	500 Gbps	500 Gbps	500 Gbps	1.2 Tbps
Packets Rate (pps)*1	50 Million	50 Million	100 Million	110 Million
Software-based - SYN Authentication (pps)	50 Million	50 Million	100 Million	110 Million
Hardware-based - Anomaly Flood Blocking (pps)	250 Million	220 Million	440 Million	500 Million
Maximum Concurrent Sessions (asymmetric deployment)	64 Million	128 Million	256 Million	256 Million
Average Latency	60 µs	60 µs	60 µs	60 µs
Minimum Rate Enforcement Interval	100 ms	100 ms	100 ms	100 ms
Flow Detection Performance				
Flows Per Second (fps)	6 Million	N/A	N/A	N/A
DNS Authoritative Cache Performance				
DNS Queries Per Second (qps)	35 Million	35 Million	N/A	N/A
Network Interface				
1/10 GE Fiber (SFP+)	48	0	0	0
40 GE Fiber (QSFP+)	0	4	4	0
100 GE Fiber	4 (QSFP28)	4 (CFP2 or QSFP28)	4 (CFP2 or QSFP28)	16 (QSFP28)
Management Ports	Ethernet Mgmt Port, RJ-45 Console Port+			
Hardware Specifications				
Processor	2 x Intel Xeon 18-core	2 x Intel Xeon 18-core	4 x Intel Xeon 18-core	2 x Intel Xeon 28-core
Memory (ECC RAM)	128 GB	256 GB	512 GB	384 GB
Storage	SSD	SSD	SSD	SSD
Hardware Acceleration	3 x FTA-4, SPE	4 x FTA-3, SPE	8 x FTA-3, SPE	2 x FTA-5, SPE
Dimensions (inches)	1.75 (H) x 17.5 (W) x 30 (D)	5.3 (H) x 16.9 (W) x 30 (D)	5.3 (H) x 16.9 (W) x 30 (D)	2.625 (H) x 17.5 (W) x 30 (D)
Rack Units (mountable)	1U	3U	3U	1.5U
Unit Weight	35.7 lbs	80 lb	102 lbs	44.2 lbs
Power Supply (DC option available)	Dual 1500W RPS	2+2 1100W RPS	2+2 1100W RPS	Dual 1500W RPS
	80 Plus Platinum efficiency, 100-240 VAC, 50-60 Hz			
Power Consumption (typical/max)*2	784W / 1,078W	1,000W / 1,200W	1,700W / 2,000W	1,121W / 1,300W
Heat in BTU/Hour (typical/max)*2	2,676 / 3,679	3,412 / 4,095	5,801 / 6,825	3,826 / 4,436
Cooling Fan (front-to-back airflow)	Hot Swap Smart Fans			
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%			
Regulatory Certifications	FCC Class A, UL, CE, CB, VCCI, BSMI, RCM | RoHS	FCC Class A, UL, CE, CB, VCCI, CQC, KCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, CB, VCCI, CQC, KCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, CB, VCCI, BSMI, RCM | RoHS
Standard Warranty	90-day Hardware and Software			

Hardware specifications and performance numbers are subject to change without notice, and may vary depending on configuration and environmental conditions. As for network interface, it's highly recommended to use A10 Networks qualified optics/transceivers to ensure network reliability and stability.

*1 Throughput performances are traffic-forwarding capacity and measured with legitimate traffic with DDoS protection enabled.
*2 With base model | *3 10Gbps speed only | *4 Optional RPS available | *5 Fixed SFP+ optical ports with dual rate (10GBASE-SR and 1000BASE-SX) | *6 Active CPU core counts and memory size may vary depending on the modular license | ^ Certification in process | + Thunder 14045 comes with a splitter cable for console to provide access to both modules

Thunder TPS Virtual Appliance Specifications

vThunder TPS	
Supported Hypervisors	VMware ESXi 6.7 or higher (SR-IOV)
Hardware Requirements	See Installation Guide
Standard Warranty	90-day Software

vThunder TPS License and Sizing Recommendations

Throughput	Lab/1/2/5 Gbps	40 Gbps*1	100 Gbps*2
vCPU	6	8	24
vRAM	16 GB	32 GB	64 GB
vDisk	60 GB	60 GB	100 GB
Licence Types	Bandwidth license (per instance)	FlexPool	FlexPool
Hypervisors	ESXi	ESXi	ESXi

*1 Available in ACOS 6.0 and above. Tested with vThunder TPS running on ESXi with Intel XL-710 NIC (SR-IOV enabled)
*2 Available in ACOS 6.0 and above. Tested with vThunder TPS running on ESXi with NVIDIA Mellanox ConnectX-5 NIC (SR-IOV enabled)

vThunder TPS Detector Flow Detection Performance*

Flows per Second (fps)	150K	500K	1.5M
vCPU	2	3	5
vRAM	16 GB	32 GB	64 GB
vDisk	40 GB	40 GB	40 GB

* Using vThunder TPS Standalone Detector image.

Thunder TPS for Cloud

	Microsoft Azure
Throughput per instance	Up to 5 Gbps
Image Format	Microsoft VHD
Licenses	30-day Trial License | BYOL FlexPool License

Detailed Feature List

Features may vary by appliance.

Detection/Analysis

- In-line packet-based DDoS detection
- Out-of-band flow-based DDoS detection
- Distributed detection
- Individual detection policies for more than 256K servers and services
- Continuous behavioral learning
- Manual and learned thresholds
- Protocol anomaly detection
- Inspection within IPinIP (e.g., networking, encapsulation)
- Black/white lists
- Traffic indicator and top talkers
- Mitigation console
- Packet debugger tool
- Top-k insights (source, destination)
- Outbound detection
- Victim IP Identification

DDoS Threat Intelligence Service

- Dynamically updated threat intelligence feed
- IP addresses of open reflector or amplification weapons
- IP addresses of DDoS botnets

Zero-day Automated Protection

- ZAPR: Machine learning powered attack pattern recognition and filtering
- TCP progression tracking
- Prevent zero-day attacks
- No pre-configuration or manual intervention
- Fast, automated response

Resource Attack Protection

- Fragmentation attack
- Slowloris
- Slow GET/POST
- Long form submission
- SSL renegotiation

Application Attack Protection

- Application-aware filter
- Regular expression filter (TCP/UDP/HTTP/SIP)
- HTTP request rate limit (per URI)
- DNS request rate limit (per type, FQDN, label count)
- SIP request limit (per type)
- Application request malformed check (DNS/HTTP/SIP)
- DNS domain-list
- HTTP/S protocol compliance
- Application (DNS/HTTP/SIP) flood protection
- Signature-based IPS
- QUIC version control and malformed header check
- Packet watermarking (UDP) for gaming traffic

Protocol Attack Protection

- Invalid packets
- Anomalous TCP flag combinations (no flag, SYN-FIN, SYN frag, LAND attack)
- SYN-ACK amplification attack protection
- IP options
- Packet size validation (ping of death)
- POODLE attack
- TCP/UDP/SSL/ICMP flood protection
- Per-connection traffic control

Challenge-based Authentication

- TCP SYN cookies, SYN authentication
- ACK authentication
- Spoof detection
- DNS authentication
- HTTP challenge

Protected Objects

- Protected zones for automated detection and mitigation
- Source/destination IP address/subnet
- Source and destination IP pair
- Destination port
- Source port
- Protocol (e.g., HTTP, DNS, SIP, TCP, UDP, ICMP and others)
- Class list/geolocation
- Passive mode
- Outbound mitigation symmetric deployment

Non-stop DNS Solution

- Act as Authoritative DNS cache
- Seamless layered protection with TPS mitigation
- DNS water torture protection
- Selective and customizable response/ forward

Actions

- Capture packet
- Run script
- Drop
- TCP reset
- Dynamic authentication
- Add to black list
- Add to white list
- Log
- Limit concurrent connections
- Limit connection rate
- Limit traffic rate (pps/bps)
- Forward to other device
- Remote-triggered black hole (RTBH)
- BGP Flowspec

Management

- Dedicated on-box management interface (GUI, CLI, SSH, Telnet)
- aGalaxy for comprehensive management
- SNMP, syslog, email alerts
- REST API (aXAPI) or SDK
- LDAP, TACACS+, RADIUS support
- Configurable control CPUs

Networking and Deployment

- Proactive, Reactive, Asymmetric, Symmetric, Out-of-band (TAP)
- Transparent (L2), routed (L3)
- Virtual wire
- Routing: static routes, BGP4+, OSPF, OSPFv3, IS-IS
- Bidirectional forwarding detection (BFD)
- VLAN (802.1Q)
- Trunking (802.1AX), LACP
- Access control lists (ACLs)
- Network Address Translation (NAT)
- MPLS traffic protection
- BGP route injection,
- BGP FlowSpec
- IPinIP (source and terminate)
- GRE tunnel interface
- VXLAN

Detailed Feature List (Cont.)

Telemetry

- Rich traffic and DDoS statistics counters
- sFlow v5
- NetFlow (e.g., v9, IPFIX)
- Custom counter blocks for flow-based export
- High-speed logging
- CEF logging

High-performance, Scalable Platform

- Advanced Core Operating System (ACOS)
- Linear application scaling
- ACOS on data plane
- Linux on control plane
- IPv6 feature parity
- Security policy engine (SPE) enabling hardware acceleration for policy enforcement*
- High-performance hardware blocking*

Carrier-grade Hardware*

- Advanced hardware architecture
- Hot-swap redundant power supplies (AC and DC)
- Smart fans (hot swap)
- Solid-state drive (SSD)
- Tamper detection
- 40 GbE and 100 GbE ports

Security and Capability Assurance Certifications*

- Common Criteria EAL 2+
- FIPS 140-2 Level 2 Compliance (Thunder 14045)
- FIPS 140-1 Level 1 Compliance (all)

* Features and certifications may vary by appliance.

Learn More

About A10 Networks

Contact Us

A10networks.com/contact

Part Number: A10-DS-15101-EN-34 March 2023